



UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/015,902	10/30/2001	Sanguthevar Rajasekaran	028410-0017	5784

29580 7590 10/05/2005

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
ATTN: JAN STEELE
525 UNIVERSITY AVENUE
SUITE 1100
PALO ALTO, CA 94301

EXAMINER

PARTHASARATHY, PRAMILA

ART UNIT PAPER NUMBER

2136

DATE MAILED: 10/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/015,902

Applicant(s)

RAJASEKARAN ET AL.

Examiner

Pramila Parthasarathy

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 11 July 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-66 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-66 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

AT

DETAILED ACTION

Specification

1. The new title is clearly indicative of the invention to which the claims are directed and is entered.
2. Objection to the disclosure is hereby withdrawn and request for correction to the U.S. Publication 20020083327 has been entered.

Claim Rejections - 35 USC § 112

3. Claims 1 – 50 and 52 – 66 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

The amended independent Claims 1, 6, 39, 42, 52 and 54 – 66 read, “ ... generating a bogus secret configured to camouflage said secret....”, Claims 11 and 45 reads, “... generating a bogus matrix configured to camouflage the matrix....”, Claim 24, 48 and 53 reads, “... generating a bogus state information to camouflage said state

information....”, “...bogus candidate state information...”, and Claim 7 reads, “... said bogus secret”.

With respect to “generating a bogus secret configured to camouflage said secret”, although the specification discloses “If the user further attempts to use the “bogus” form of the secured object” and “...but instead causes to be entered a dummy or otherwise bogus graph, G...” (See instant application pages 9, 20 and 26), the specification does not disclose “generating a bogus secret configured to camouflage said secret”. The specification does not indicate how to “generating a bogus secret configured to camouflage said secret” is carried out. Applicant amendment does not clarify the steps of generating a bogus secret configured to camouflage said secret.

With respect to “generating a bogus matrix configured to camouflage the matrix”, although the specification discloses “If the user further attempts to use the “bogus” form of the secured object” and “...but instead causes to be entered a dummy or otherwise bogus graph, G...” (See instant application pages 9, 20 and 26), the specification does not disclose “generating a bogus matrix configured to camouflage the matrix”. The specification does not indicate how to “generating a bogus matrix configured to camouflage the matrix” is carried out. Applicant amendment does not clarify the steps of generating a bogus matrix configured to camouflage the matrix.

With respect to “generating a bogus state information to camouflage said state information” and “...bogus candidate state information...”, although the specification

discloses “If the user further attempts to use the “bogus” form of the secured object” and “...but instead causes to be entered a dummy or otherwise bogus graph, G....” (See instant application pages 9, 20 and 26), the specification does not disclose “generating a bogus state information to camouflage said state information” and “...bogus candidate state information...”. The specification does not indicate how to “generating a bogus state information to camouflage said state information” or “...bogus candidate state information...” is carried out. Applicant amendment does not clarify the steps of generating a bogus state information to camouflage said state information or “...bogus candidate state information...”.

With respect to “bogus secret”, although the specification discloses “If the user further attempts to use the “bogus” form of the secured object” and “...but instead causes to be entered a dummy or otherwise bogus graph, G....” (See instant application pages 9, 20 and 26), the specification does not disclose “bogus secret”. The specification does not indicate how to “bogus secret” is carried out. Applicant amendment does not clarify bogus secret.

For Examination purposes, “generating a bogus secret/matrix/state information” will be broadly interpreted as **generating a secret** (emphasis added).

The dependent claims 2 – 5, 8 – 10, 12 – 23, 25 – 38, 40, 41, 43, 44, 46 and 47 are rejected at least by virtue of their dependency on the dependent claims.

Claims 1, 6, 11, 24, 39, 42, 45, 48 and 52 – 66, recite the limitation "said secret" in claim limitation "...regenerating said secret if said candidate password...". There is insufficient antecedent basis for this limitation in the claim. Usage of "said secret" is ambiguous and does not clarify whether it is "bogus secret" or "candidate secret".

The dependent claims 2 – 5, 7 – 10, 12 – 23, 25 – 38, 40, 41, 43, 44, 46 and 47 are rejected at least by virtue of their dependency on the dependent claims.

Response to Arguments

4. Applicant's arguments filed 7/11/2005 have been fully considered but they are not persuasive.

Applicant agrees with the Examiner that the cited prior arts (CPA) [Eldridge et al. U.S. Patent 6,061,799, hereinafter "Eldridge"], disclose an authentication system where a user gains access to a network through the use of passwords and public and private keys; a server reading a client identifier from a medium and then compares the client identifier to a database on the server; generate authentication data and that the authentication system compares the key with a database of keys before access to the server is allowed.

Examiner would like to specifically point out that even though Claim 51 designation says "currently amended", amendment filled on 7/11/2005 does not reflect any such amendments to Claim 51. For examination purposes, Claim 51 reads as filled on 10/30/2001.

Regarding currently amended claims 1, 6, 7, 11, 24, 39, 42, 45, 48 and 52 – 66, Applicant argues that Eldridge does not teach “generating a bogus secret configured to camouflage said secret....”, “...bogus candidate state information...”, “... generating a bogus matrix configured to camouflage the matrix....”, “... generating a bogus state information to camouflage said state information....”, and “... said bogus secret”. These arguments are not found persuasive. Eldridge discloses “generating a bogus secret configured to camouflage said secret....”, “... generating a bogus matrix configured to camouflage the matrix....”, “... generating a bogus state information to camouflage said state information....”, and “... said bogus secret”, as broadly interpreted above, the server reads the secret (password) to generate authentication data, i.e., a key and only that key is accepted for the authorization challenge (Summary and Column 10 lines 23 – 50).

Therefore, the examiner respectfully asserts that the cited prior art does teach or suggest the amended subject matter “generating a bogus secret configured to camouflage said secret....”, “...bogus candidate state information...”, “... generating a bogus matrix configured to camouflage the matrix....”, “... generating a bogus state information to camouflage said state information....”, and “... said bogus secret”. broadly recited in the amended independent claims 1, 6, 7, 11, 24, 39, 42, 45, 48 and 52 – 66. The dependent claims 2 – 5, 8 – 10, 12 – 23, 25 – 38, 40, 41, 43, 44, 46 and 47 are rejected at least by virtue of their dependency on the dependent claims and by other reason set forth in this office action. Accordingly, the rejection for the pending claims 1 – 66 is respectfully maintained.

Claim Rejections - 35 USC § 102

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

5. Claims 1, 2, 5 – 7, 10 – 12, 24, 26, 39, 42, 45, 48 and 51 – 66 are rejected under 35 U.S.C. 102(a) as being anticipated by Eldridge et al. (U.S. Patent Number 6,061,799).

6. Regarding Claims 1, 39, 51 and 55, Eldridge teaches and describes a method for operating an access control system to camouflage a secret so as to be accessible by an authorized user yet protected against unauthorized access, said method comprising the steps of:

(a) representing in digital form a secret to be protected against unauthorized access (Column 4 lines 64 – Column 5 line 7);

(b) storing a plurality of computer-represented objects related to said secret (Column 4 line 64 – Column 5 line 7);

(i) at least one of said objects being accessible by an authorized user as a password (Column 5 lines 7 – 9);

(ii) at least another of said objects being stored in a computer-readable wallet accessible to said access control system (Column 5 lines 7 – 9 and Column 8 line 63 – Column 9 line 13); and

(c) representing said secret as a function of said plurality of objects, using a

composition function (Column 5 lines 4 – 18 and 57 – 65); and

(d) storing, in a computer-readable memory, said composition function:

(i) in a manner accessible to said access control system (Column 8 line 63 – Column 9 line 13);

(ii) so as to be executable to generate a candidate secret using a user-inputted candidate password in conjunction with at least said another object stored in said wallet (Column 9 line 5 – 22);

(iii) generating a bogus secret configured to camouflage said secret if said candidate password is not said password (Column 9 lines 36 – 52 and Column 10 line 23 – 50), Eldridge teaches the key is generated only if the password is authorized; and

(iv) regenerating said secret if said candidate password is said password (Column 9 lines 36 – 52 and Column 10 lines 23 – 50);

thereby protecting said secret against unauthorized access by camouflaging the secret from persons not having said password.

7. Regarding Claims 6, 42, 52 and 56, Eldridge teaches and describes a method for operating an access control system to release a secret camouflaged to be accessible to an authorized user yet protected against unauthorized access, said method comprising the steps of:

(a) accessing a plurality of computer-represented objects related to a secret (Column 7 lines 19 – 22);

(i) at least one of said objects being accessible by an authorized user as a

password (Column 5 lines 7 –9);

(ii) at least another of said objects being stored in a computer-readable wallet accessible to said access control system (Column 5 lines 7 – 9 and Column 8 line 63 – Column 9 line 13); and

(b) accessing a composition function representing said secret as a function of said plurality of objects (Column 9 lines 36 – 43);

(c) receiving a candidate password inputted by a user (Column 7 lines 8 – 10);

(d) generating a candidate secret for said user by executing said composition function using as operands thereto said candidate password in conjunction with at least said another object stored in said wallet (Column 5 line 56 – Column 6 line 11);

(i) generating a bogus secret configured to camouflage said secret if said candidate password is not said password (Column 9 lines 36 – 52 and Column 10 line 23 – 50), Eldridge teaches the key is generated only if the password is authorized; and

(ii) regenerating said secret if said candidate password is said password (Column 9 lines 36 – 52 and Column 10 lines 23 – 50);

(e) outputting said candidate secret to said user of said access control system (Column 9 line 64 – Column 10 line 11).

8. Regarding Claim 11, 45, 53, 54, 57, 59, 60, 63 and 64, Eldridge teaches and describes a method for operating an access control system to protect state information against unauthorized access, said method comprising the steps of:

(a) obtaining state information represented in digital form (Column 5 lines 7 – 9 and Column 8 lines 15 – 19);

(b) deriving from said state information a first matrix (Column 5 lines 7 – 9 and Column 8 lines 19 – 24);

(c) storing said first matrix as a password usable by an authorized user (Column 4 line 64 – Column 5 line 7);

(d) deriving from said state information a second matrix (Column 5 lines 7 – 9 and Column 8 lines 15 – 19);

(e) storing said second matrix in a computer-readable wallet accessible to said access control system (Column 5 lines 7 – 9 and Column 8 line 63 – Column 9 line 13); and

(f) storing, in a computer-readable memory, a composition function executable to generate a candidate matrix using a user-inputted candidate password in conjunction with said second matrix (Column 9 lines 5 – 22);

(i) generating a bogus matrix configured to camouflage said matrix if said candidate password is not said password (Column 9 lines 36 – 52 and Column 10 line 23 – 50), Eldridge teaches the key is generated only if the password is authorized; and

(ii) regenerating said matrix if said candidate password is said password (Column 9 lines 36 – 52 and Column 10 lines 23 – 50);

thereby protecting said secret against unauthorized access by camouflaging said matrix from persons not having said password.

Art Unit: 2136

9. Regarding Claim 24, 48, 58, 61, 62, 65 and 66, Eldridge teaches and describes a method for operating an access control system to protect state information against unauthorized access, said method comprising the steps of:

(a) retrieving a first matrix related to said state information from a computer-readable wallet accessible to said access control system (Column 7 lines 19 – 22 and Column 8 lines 15 – 19);

(b) accessing a composition function representing said state information as a function of said first matrix and a password stored as a second matrix (Column 9 lines 36 – 43);

(c) receiving a candidate password inputted by a user (Column 7 lines 8 – 10);

(d) generating candidate state information for said user by executing said composition function using as operands thereto said candidate password in conjunction with at least said first matrix stored in said wallet ((Column 5 line 56 – Column 6 line 11 and Column 9 lines 5 – 22);

(i) generating a bogus state information to camouflage said state information if said candidate password is not said password (Column 9 lines 36 – 52 and Column 10 line 23 – 50), Eldridge teaches the key is generated only if the password is authorized; and

(ii) regenerating said state information if said candidate password is said password (Column 9 lines 36 – 52 and Column 10 lines 23 – 50);

thereby protecting said secret against unauthorized access by camouflaging the secret from persons not having said password.

(e) outputting said candidate state information or bogus candidate state information to said user of said access control system (Column 9 line 64 – Column 10 line 11).

10. Claims 2 and 12 are rejected as applied about in rejecting Claims 1 and 11. Furthermore, Eldridge teaches and describes a method for operating an access control system to camouflage a secret so as to be accessible by an authorized user yet protected against unauthorized access, further comprising effecting a multilevel camouflaging scheme by camouflaging said at least another object stored in said wallet (Column 5 lines 56 – 67).

11. Claims 5 and 10 are rejected as applied about in rejecting Claims 1 and 11. Furthermore, Eldridge teaches and describes a method for operating an access control system to camouflage a secret so as to be accessible by an authorized user yet protected against unauthorized access, where:

(i) said secret is a private key of said user (Column 5 lines 18 – 22 and Column 6 lines 1 – 11);

(ii) said object accessible by said user is a PIN of said user (Column 5 lines 25 – 29);

(iii) said another object stored in said wallet is a pseudo-valid PIN (Column 7 lines 10 – 14); and

(iv) said candidate secret has the structural form of a private key (Column 5 lines 35 – 55).

12. Claim 7 is rejected as applied about in rejecting Claim 6. Furthermore, Eldridge teaches and describes a method for operating an access control system to camouflage a secret so as to be accessible by an authorized user yet protected against unauthorized access, where in said step (d)(i) said bogus secret is configured to deceive an unauthorized user into believing that said bogus secret is said secret (Column 5 lines 30 – 39).

13. Claim 26 is rejected as applied about in rejecting Claim 24. Furthermore, Eldridge teaches and describes a method for operating an access control system to camouflage a secret so as to be accessible by an authorized user yet protected against unauthorized access, where at least one of said matrices is stored on a smart card accessible to said user (Column 5 lines 4 – 14).

Claim Objections

14. Claims 3, 4, 8, 9, 13 – 23, 25, 27 – 38, 40, 41, 43, 44, 46, 47, 49 and 50 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

21. Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant.

Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

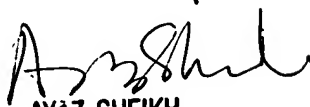
22. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Applicant is urged to consider the references. However, the references should be evaluated by what they suggest to one versed in the art, rather than by their specific disclosure. If applicants are aware of any better prior art than those are cited, they are required to bring the prior art to the attention of the examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
October 02, 2005.


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100